JOHN S. LEONARDO
United States Attorney
District of Arizona
FREDERICK A. BATTISTA
Maryland State Bar Member
PETER S. SEXTON
Arizona State Bar No. 011089
JAMES R. KNAPP
Arizona State Bar No. 021166
Assistant U.S. Attorneys
Two Renaissance Square
40 N. Central Ave., Suite 1200
Phoenix, Arizona 85004
Telephone: (602) 514-7500
Fred.Battista@usdoj.gov
Peter.Sexton@usdoj.gov
James.Knapp2@usdoj.gov
Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZONA

United States of America, Plaintiff, vs. Daniel David Rigmaiden, Defendant.	CR-08-0814-PHX-DGC **GOVERNMENT'S RESPONSE TO DEFENDANT'S MOTION FOR RECONSIDERATION**

The United States, through undersigned counsel, opposes Defendant's motion for reconsideration under Local Rule 7.2(g). "Motions for reconsideration 'are disfavored and will be granted only upon a showing of manifest error or new facts or legal authority which could not have been raised earlier with reasonable diligence.' Mere disagreement with an order is an insufficient basis for reconsideration. Nor should a motion for reconsideration be used to ask the Court to rethink its analysis." Ariz. Dream Act Coalition v. Brewer, ___ F. Supp. 2d ___, 2013 WL 2128315 at *25 (D. Ariz. May 16, 2013).

As argued below, Defendant fails to show any manifest error or new facts or law that would affect the Court's May 8, 2013, Order denying his motion to suppress.

Accordingly, his motion for reconsideration should be denied.

I. Defendant's Alleged Manifest Factual Errors.

1. Use Of False Identities. Defendant fails to identify any errors that would affect the reasoning in the Court's May 8, 2013, Order. Defendant used numerous false identities, and the driver's license numbers he provided were assigned to real people. Furthermore, evidence provided in discovery shows that Defendant operated a website (www.fakeid.tv) where he sold fake California driver's licenses. See also CR 845-1 (search warrant affidavit for apartment) at 24 ¶ 27. Defendant fails to explain why it matters, for purposes of deciding the motion to suppress, whether he knew the numbers he used were already assigned to real people.

2. Abandonment Of Apartment. Defendant again fails to identify any error. The Court may draw inferences from the available evidence when considering a motion to suppress. See United States v. Williams, 630 F.2d 1322, 1327 (9th Cir. 1980); see also United States v. Cervantes-Gaitan, 792 F.2d 770, 772 (9th Cir. 1986). Defendant admitted in a declaration that he used a false identity to rent the apartment, and that if he had learned of law enforcement's attempts to locate the aircard he would have cleared out of the apartment within a day and stopped using the aircard. See CR 824-2 at ¶¶ 3, 14. That alone amply supports the Court's finding that Defendant was prepared to abandon the apartment and flee. If more were needed, the Court could consider Defendant's boasts about additional countermeasures he had planned as well as his actual flight when law enforcement attempted to arrest him, as detailed in the search warrant affidavits. See, e.g., CR 845-1 (search warrant affidavit for apartment) at 46-48 ¶¶ 91, 93, 100 (countermeasures), 51 ¶ 108(i) (flight).

3. Cash, Passport, And Backup Computer In Storage Unit. The storage unit contained an external hard drive with an encrypted backup copy of contents of his laptop. In addition to quibbling over whether an external hard drive is a computer, Defendant continues to quibble over whether a 24-hour escape is a "quick escape," but he fails to

identify any factual errors that would affect the reasoning in the Court's Order.

4. Travis Rupard Aircard. Defendant claims that he purchased the aircard without providing any name. The United States obtained no information during the investigation about the actual purchase of the aircard. Nevertheless, Defendant activated the aircard and maintained the aircard under the false identity Travis Rupard, which is the name listed in Verizon's subscriber records.

5. Fraudulent Andrew Johnson Visa Card. Defendant is correct that the Visa card was tied to a prepaid account, but the fact remains: he used a fraudulent visa card obtained through the use of a deceased person's name and social security number to purchase the laptop. There is no error.

6. Investigation Of Defendant's False Identities. Defendant again identifies no specific error or modification sought. To the extent it matters, the United States had already attempted to peel back some of the layers of false identities (including "Travis Rupard" and "Patrick Stout") before it began the aircard tracking operation.

7. Sending Signals To Aircard As "Severe Intrusion." Defendant identifies no specific error or modification sought.

8. Expunction Of Data. Defendant does not dispute that the data was expunged. He speculates that the FBI had improper motives in doing so, but the United States has provided a declaration from an FBI supervisory agent as well as an excerpt of the relevant FBI policy to show that it is, in fact, routinely done at the conclusion of a tracking operation. See CR 674-1 (declaration). Defendant identifies no specific error or modification sought.

9. New Technology And Lack Of Legal Precedent. In the Fourth Amendment context, cell phone tracking is relatively new technology and there is—and certainly was in 2008—a lack of legal precedent. Defendant identifies no specific error or modification sought.

10. Gate Access Records. Defendant identifies no specific error or modification

sought.

11. Encrypted Data. Defendant identifies no specific error or modification sought.

12. Search Incident To Arrest. The Court's description is correct: "After a foot chase through the surrounding area, Defendant was apprehended by local police officers who happened to be on the scene. Agents searched the suspect incident to his arrest and found a set of keys in his pocket." CR 1009 at 5. The local law enforcement officers were acting at the express request for assistance from federal agents armed with a federal arrest warrant. Federal agents were present during the arrest. It is of no consequence to the motion to suppress who actually found the keys.

13. Search Of Apartment. Again, the Court's description is correct: "An agent took the keys to unit 1122 and confirmed that they fit and turned the door lock. The agent waited for the arrival of other agents with the search warrant before entering the apartment." CR 1009 at 5. It does not appear that the agent who took the keys to Unit 1122 ever entered the apartment, but he certainly did not do so before the arrival of the warrant and the search team.

II. Manifest Legal Errors.

A. Execution Of Tracking Warrant. Defendant first argues that the Court overlooked his arguments that the tracking warrant was not executed by the FBI. The United States is unable to discern Defendant's argument on this issue.

B. Independent Searches And Seizures. Defendant also argues that the Court overlooked the independent searches and seizures involved in the aircard tracking operation and ignored all of his arguments about the scope of the Fourth Amendment search and seizure. In making this argument, however, Defendant overlooks the distinction between 1) analyzing at the outset whether the warrant was sufficiently particular to authorize the aircard tracking operation, and 2) analyzing after the fact whether the warrant was executed reasonably in light of the Fourth Amendment. The

warrant must specify the aircard to be located, but, under Dalia v. United States, it need not specify the precise manner in which the warrant would be executed. See 441 U.S. 238, 257 (1979).

Here, the Court concluded that the warrant was sufficiently particular, and it properly relied on Dalia to reject Defendant's argument that the warrant failed to specify the various searches and seizures that might occur during its execution. See CR 1009 at 25-27 & n.7. The Court also concluded that the aircard tracking operation was not a severe intrusion, even assuming all of Defendant's allegations were true. See CR 1009 at 13; see also CR 873 (Gov't Resp. Mot. Suppress) at 53-54 (citing cases on reasonableness of execution). Thus, the Court properly considered and rejected Defendant's scope arguments.

C. Use Of Two Devices. Similarly, Defendant argues that the warrant only authorized the use of one device, not two. The Court already rejected this argument. CR 1009 at 24-25. Moreover, United States v. Chen, 979 F.2d 714 (9th Cir. 1992), which Defendant cites in his motion for reconsideration, provides no support for his argument. In Chen, the Ninth Circuit concluded that the use of multiple cameras for video surveillance was "motivated by considerations of practicality rather than by a[n improper] desire to engage in indiscriminate 'fishing,'" and it reversed the district court's suppression of the video evidence. 979 F.2d at 718. Here, the use of two devices at different times rather than a single device simply allowed the FBI to execute the warrant; it did not broaden the scope of what was to be accomplished (that is, locate the aircard).

D. Authorization To Use Mobile Tracking Device. Defendant further argues that the warrant did not authorize anyone to use a mobile tracking device to locate his aircard, citing United States v. Robinson, 358 F. Supp. 2d 975 (D. Mont. 2005). Robinson is irrelevant. In Robinson, the warrant authorized the search of a pickup truck but it failed to explicitly authorize the search of a related residence. See 358 F. Supp. 2d at 977 & n.2. The district court suppressed evidence obtained from the residence because the warrant

did not authorize the search of that location with particularity, as required by the Fourth Amendment. Id. at 980-981. But see Kennith J. Melilli, What Nearly A Quarter Century Of Experience Has Taught Us About Leon And "Good Faith," 2008 Utah L. Rev. 519, 554-555 (2008) (criticizing Robinson). Here, however, the warrant described the aircard to be tracked with particularity, including its description, telephone number, and ESN number. As explained in the Court's Order, the manner in which the warrant would be executed—including the equipment that law enforcement might use—need not be precisely described. See CR 1009 at 25-27.

E. Dalia v. United States And New Technology. Defendant argues that Dalia v. United States does not apply to searches and seizures using new technology, but neither of his cases even cite Dalia. See United States v. Oliva, 705 F.3d 390, 399 (9th Cir. 2012) (rejecting motion to suppress based on defendant's allegation that wiretap authorized "unlawful roving bugs"); In Re Warrant To Search A Target Computer At Premises Unknown, 2013 WL 1729765 (S.D. Tex. Apr. 22, 2013) (denying warrant application).

F. Incorporation Of Affidavit By Reference. Defendant argues that the Court improperly considered the affidavit. To the extent the Court even needs to consider the affidavit, the case Defendant cites—United States v. SDI Future Health, Inc.—supports the Court's analysis. See 568 F.3d 684, 699 (9th Cir. 2009) (holding that language "noting 'the supporting affidavit(s)' as the 'grounds for application for issuance of the search warrant'" is sufficient to incorporate by reference); id. at 701 n.10 (stating that "we have never required actual reliance on an affidavit to meet the second prong for incorporation into a warrant").

G. Computer Search Protocol. Defendant complains that law enforcement agents' review of his computer was too thorough. In particular, he complains that law enforcement reviewed information outside of the date range on the warrant.

The warrant authorizes the seizure of evidence relating to "possible violations of

the following [enumerated] statutes . . . [f]or the period January 1, 2005, through the present." See CR 845-2 (search warrant for apartment) at 4. This temporal limitation applies to the violations being investigated, not the type of evidence that may be relevant. For example, electronic copies of identity theft evidence, such as birth certificates or lists of social security numbers, would have plainly been within the scope of the warrant, even if those electronic copies were created prior to January 1, 2005. See CR 845-2 (search warrant for apartment) at 6 ¶ 3 ("Records . . . containing personal identifiable information on indviduals, whether living, deceased or fictictious . . . who may have been a victim of identity theft"). Moreover, date stamps on computer files can sometimes be unreliable. Law enforcement was under no obligation to ignore digital evidence date-stamped prior to January 1, 2005.

Defendant also argues that the Court "ignored binding Ninth Circuit precedent" in Marks v. Clarke, 102 F.3d 1012 (9th Cir. 1996), when it found that the United States acted in good faith in its interpretation of the computer search protocol. See CR 1033 at 32. Marks sheds very little light on the issue before this Court, as it deals with a separate issue: qualified immunity for officers who executed a facially invalid warrant. Id. at 1028. In Marks, police officers executed a general warrant that authorized the search of all people present at two locations without probable cause. Id. at 1026. Here, in contrast, the search warrant particularly described the items to be seized and there was ample probable cause to believe that evidence would be found on the computers. The protocol at issue did not undermine the validity of the warrant; it merely set forth procedures to follow in its execution. See CR 845-2 at 14-16.

In addition, Defendant re-argues many of the same points he made in his prior voluminous pleadings, which have already been considered and rejected by the Court.

H. Reasonable Expectation Of Privacy. The United States agrees with the Court's decision that this defendant in this case lacks a reasonable expectation of privacy in the apartment, laptop, and aircard. Defendant challenges the Court's finding of facts in

support of its decision. CR 1033 at 38. The United States recognizes that there is no evidence in the record regarding the source or sources of funds for the purchase of the aircard, the maintenance of the aircard account, the payment of rent, etc., and that a hard drive and not a computer was found in defendant's storage unit. The Court's original findings of fact read as follows:

> The Court concludes that Defendant's presence in the apartment was wrongful in the same sense as the burglar's discussed in *Rakas*. Virtually everything about Defendant's actions related to the apartment was fraudulent. Defendant rented the apartment using the name of a deceased individual, provided a forged California driver's license to support the false identity, used the drivers' license number from another person in support of the forged license, and provided a forged tax return to support his purported ability to pay rent. Defendant used the laptop he had procured through fraud in the apartment, and connected to the Internet with the aircard purchased with a false identity while using the account with Verizon that he maintained using a false identity. Even the electricity that lighted the apartment and powered the computer and the aircard was purchased in a false name. What is more, while living in the apartment under false pretenses, Defendant had $70,000 in cash, a false passport, and a copy of his laptop computer in a storage unit (also rented under false pretenses) ready for a quick escape.

CR 1009 at 9-10. However, since defendant has offered a proposed amended set of findings with respect to this issue, see CR 1033 at 38, the United States offers the following proposed amended set of findings of facts as well:

> The Court concludes that Defendant's presence in the apartment was wrongful in the same sense as the burglar's discussed in *Rakas*. Virtually everything about Defendant's actions related to the apartment was fraudulent. Defendant rented the apartment using the name of **Steven Brawner (False Identity #1),** a deceased individual, provided a forged California driver's license to support the false identity, used the **valid** drivers' license number from another person **(False Identity #2)** in support of the forged license, and provided a forged tax return to support his purported ability to pay rent. Defendant used the laptop he had procured through fraud **in that he purchased it through the use of a Visa card account obtained and maintained using the name of Andrew Johnson, a deceased individual (False Identity #3)** in the apartment, and connected to the Internet with the aircard purchased **by defendant** with a false identity while using the account with Verizon that he maintained using a false identity **of Travis Rupard, a living individual (False Identity #4)**. Even the electricity that lighted the apartment and powered the computer and the aircard was purchased in a false name, **Brawner**. What is more, while living in the apartment under false pretenses, Defendant had $70,000 in cash, a false **facially valid U.S.** passport **Defendant had obtained using his Andrew Johnson false identity**, and a copy **on a hard drive** of **all of**

> **his primary fraudulent identity and fraudulent scheme programs Defendant also maintained on** his laptop computer in a storage unit (also rented under false pretenses **under the name of Daniel Clifton Aldrich, a deceased person (False Identity #5**) ready for a quick escape. **By Defendant's own admission, had he become aware of law enforcement's interest in him, he would have vacated his apartment within 24 hours. There is little doubt the contents of the storage unit would have aided a relocation by Defendant on short notice and the reestablishment of his criminal operations under an identity other than Steven Brawner.**

Taken as a whole, the depth and breadth of defendant's fraudulent conduct appear to have never been considered by a court before. In an earlier stage of the litigation in this case, the United States did state "Defendant still had a reasonable expectation of privacy in the apartment itself, even though he rented it under an assumed identity, because the apartment complex had not yet discovered the fraud and attempted to evict him." See CR 465 at 22 n.3 (citing United States v. Cunag, 386 F.3d 888 (9th Cir. 2004)). The United States also noted Cunag in its response to Defendant's Motion to Suppress. See CR 873 at 57. This being said, as the United States continued to work through this issue as presented through the voluminous and extensive factual and legal arguments brought by Defendant, its thinking and arguments were refined in the course of further research and consideration of the relevant facts. As a consequence at this time, the United States believes that the Court's decision in this case is the correct one, the singular fraudulent conduct in Cunag pales in comparison to Defendant's fraudulent conduct in this case. Fraudulent conduct which in turn facilitated the ongoing violation of the privacy of many others through the assumption of their identities in order to file fraudulent tax returns and the secret use of innocent third parties' personal computers via botnets and/or proxies. In this case, under these facts, the Court's findings with respect to defendant's lack of any reasonable expectation of privacy are appropriate.

I. Objections To Pen/Trap Order, No. 08-90331. Defendant argues that the Court ignored his arguments regarding the hybrid order, No. 08-90331, but he fails to explain how this should affect the Court's Order.

J. Alleged Destruction Of Evidence. Defendant also argues that the Court

ignored the arguments in one of his supplemental memoranda, CR 830-2, but he does not explain how this should affect the Court's Order.

III. Conclusion.

As argued above, Defendant fails to show any manifest error or new facts or law that would affect the Court's May 8, 2013, Order denying his motion to suppress. Accordingly, his motion for reconsideration should be denied.

Respectfully submitted this 21st day of June, 2013.

JOHN S. LEONARDO
United States Attorney
District of Arizona

s/ Frederick Battista

FREDERICK A. BATTISTA
PETER S. SEXTON
JAMES R. KNAPP
Assistant U.S. Attorneys

CERTIFICATE OF SERVICE

I hereby certify that on 6/21/2013, I electronically transmitted the attached document to the Clerk's Office using the CM/ECF System for filing a copy to the following CM/ECF registrant:

Philip Seplow
Shadow Counsel for Defendant Daniel David Rigmaiden

A copy of the attached document was also mailed to:

Daniel David Rigmaiden
Agency No. 10966111
CCA-CADC
PO Box 6300
Florence, AZ 85132

s/ James Knapp
U.S. Attorney's Office